Julia Robinson の formula について (体のモデル理論とその応用)

AUTHOR(S):

福崎, 賢治

CITATION:

福崎, 賢治. Julia Robinson の formula について(体のモデル理論とその応用). 数理解析研究所講究録 2006, 1515: 40-49

ISSUE DATE:

2006-09

URL:

http://hdl.handle.net/2433/58699

数理解析研究所講究録
1515巻 2006年 40-49

Julia Robinsonのformulaについて

鹿児島国際大学国際文化学部　福崎賢治 (Kenji Fukuzaki)
Faculty of Intercultural Studies,
The international University of Kagoshima

1　はじめに

Julia Robinson（[1]）は1959年数体（$\mathbb{Q}$の有限次代数拡大体）の中で$\mathbb{N}$が（よって$\mathbb{Z},\mathbb{Q}$も）$\emptyset$-definableである事を示した。そこで彼女は，数体の中で非代数的整数を排除し$\mathbb{Z}$を含むformulaを巧みに構成した。言語は通常のring languageであり，そのformulaは1箇所を除き同一であり，すべての数体に通用するものである。

以下Fを数体，$\mathfrak{O}$をFの代数的整数環，$\mathfrak{p}$等は$\mathfrak{O}$の素イデアルまたは付値を示す事にする。

Theorem 1 mをすべての素イデアル$\mathfrak{p}$に対して$\mathfrak{p}^m \not| 2$となる自然数として，次の*formula*を$\varphi(a,b,t)$で表わす。

$$\exists x,y,z(1-abt^{2m}=x^2-ay^2-bz^2)$$

すると$\forall a,b\varphi(t)$はFの非代数的整数を排除する。

すなわち，任意の$t\in F\setminus\mathfrak{O}$に対してある$a,b\in F$があり，方程式$1-abt^{2m}=x^2-ay^2-bz^2$は解を$F$に持たない。

さらに，このa,bに対して，次が成り立つ。

(†)　$F\models\forall c(\varphi(a,b,c)\to\varphi(a,b,c+1))$

Fにおいて2の素因子分解は一意に定まる。そこに現われる冪指数よりも大きいmをとれば，すべての素イデアル$\mathfrak{p}$に対して$\mathfrak{p}^m \not| 2$となる。このmのみが各Fに依存する。

ここで，$\forall a,b\varphi(t)$のFにおける解集合について考えてみると，明らかに0を含むから，空集合ではない。しかし，例えば1を含むかどうか調べることも容易な事ではない。

そこでJ. Robinsonはinductive formを用いた。一般に任意のformula $\theta(t)$ に対して，formula

$$\theta(0) \wedge \forall c(\theta(c) \to \theta(c+1)) \to \theta(t))$$

を考えると，このformulaの解集合は必ずNを含んでしまう。しかしこの場合，$\theta(t)$ が非代数的整数を排除したとしても，inductive formが排除するとは限らない。

そこで，J. Robinsonは(†)を用いて，Nを含み，非代数的整数を排除するinductive formを次のように構成した。(そこでは自動的に$\mathbb{Z}$を含むことになる。)

Theorem 2 m をすべての素イデアル $\mathfrak{p}$ に対して $\mathfrak{p}^m \not| 2$ となる自然数として，次の *formula* を $\varphi(a,b,c)$ で表わす。

$$\exists x,y,z(1-abc^{2m} = x^2 - ay^2 - bz^2)$$

さらに $\psi(t)$ は次の *formula* を表わす事にする。

$$\forall a,b(\forall c(\varphi(a,b,c) \to \varphi(a,b,c+1)) \to \varphi(a,b,t))$$

すると $\mathbb{Z} \subseteq \psi(F) \subseteq \mathfrak{O}$ である。

任意の a,b に対して F で $\varphi(a,b,0)$ が成り立つから，明らかに $\psi(F) \supseteq \mathbb{N}$ であり，また F で任意の c に対して $\varphi(a,b,c) \leftrightarrow \varphi(a,b,-c)$ が成り立つから $\mathbb{Z} \subseteq \psi(F)$ である。従って $t \in F \setminus \mathfrak{O}$ を取ったとき，

$$\forall c(\varphi(a,b,c) \to \varphi(a,b,c+1)) \to \varphi(a,b,t)$$

が成り立たないような $a,b \in F$ を見つければよい。これは前の定理より出る。

J.Robinsonが証明したように，F で $\mathfrak{O}$ が $\emptyset$-definableである事は容易である。今 $a_1,\ldots,a_s$ を $\mathfrak{O}$ のintegral basisとし（ここで $s=[F:\mathbb{Q}]$），$P_i(x)$ を a_i の $\mathbb{Q}$ 上の最小多項式（従って $\mathbb{Z}$ 上の多項式）とすると，F で

$$t \in \mathfrak{O} \Longleftrightarrow \exists x_1,\ldots,x_s,y_1,\ldots,y_s(t = x_1y_1 + \cdots + x_sy_s \wedge \bigwedge_i P_i(y_i) \wedge \bigwedge_i \psi(x_i))$$

が成り立つ。

本論文では，l を奇素数とし ζ_{l^n} を1の原始 l^n 乗根とする。$F_0=\mathbb{Q}$，$n>0$ に対して $F_n=\mathbb{Q}(\zeta_{l^n})$ として，$K_l=\bigcup_n F_n$ とおくと，$F_0 \subset F_1 \subset F_2 \subset \cdots$ であり，K は $\mathbb{Q}$ の無限次Abel拡大である。$\mathfrak{O}_n$ を F_n の代数的整数環とすれば K_l の代数的整数のなす環は $\mathfrak{O}_{K_l}=\bigcup_n \mathfrak{O}_n$ である。すると，次の定理が成り立つ。

Theorem 3 次の *formula* を $\varphi(a,b,c)$ で表わす。

$$\exists x,y,z(1-abc^4=x^2-ay^2-bz^2)$$

さらに $\psi(t)$ は次の *formula* を表わす事にする。

$$\forall a,b(\forall c(\varphi(a,b,c)\to\varphi(a,b,c+1))\to\varphi(a,b,t))$$

すると $\mathbb{Z}\subseteq\psi(K_l)\subseteq\mathfrak{O}_{K_l}$ である。

2 Theorem 1の証明

次の二つの補題がキーである。F の元 b が totally positive とは b の $\mathbb{Q}$ 上共役なもののうち実なものすべてが正である事である。

Lemma 4 与えられた素イデアル $\mathfrak{p}_1$ に対して，次を満たす $\mathfrak{O}$ で互いに素な $a,b\in\mathfrak{O}$ がある。

1. $(a)=\mathfrak{p}_1\cdots\mathfrak{p}_{2k}$，ここで各 $\mathfrak{p}_i$ は相異なり，2の素因子をすべて含む。
2. b は *totally positive prime number in* $\mathfrak{O}$ で，$(a,b)_{\mathfrak{p}}=-1\iff\mathfrak{p}|a$.

Lemma 5 a,b を前の *lemma* の条件を満たすものとして，m をすべての素イデアル $\mathfrak{p}$ に対して $\mathfrak{p}^m\not|2$ となる自然数とすると，
$F\models\exists x,y,z(1-abc^{2m}=x^2-ay^2-bz^2)$ *iff* c *is a* $\mathfrak{p}$*-adic integer for all* $\mathfrak{p}$ *such that* $\mathfrak{p}|a$.

まず，上の lemma を用いて，Theorem 2 の証明を与える。

Proof of Theorem 1. 今 $t\in F\setminus\mathfrak{O}$ を取ると，ある $\mathfrak{p}_1$ に対して t は $\mathfrak{p}_1$-adic integer ではない。($\mathfrak{O}=\bigcap_{\mathfrak{p}}\mathfrak{O}_{\mathfrak{p}}$ である。$\mathfrak{O}_{\mathfrak{p}}$ は $F_{\mathfrak{p}}$ の $\mathfrak{p}$ 進整数環。) この $\mathfrak{p}_1$ に対して Lemma 3 を適用して，a,b を取る。$\nu_{\mathfrak{p}}(c+1)\geq\min(\nu_{\mathfrak{p}}(c),0)$ に注意すれば ($\nu_{\mathfrak{p}}$ は素因子 $\mathfrak{p}$ の附値)，Lemma 4 より明らかにこの a,b に対して，

$$F\models\neg\varphi(a,b,t)\wedge\forall c(\varphi(a,b,c)\to\varphi(a,b,c+1))$$

である。 □

Lemma 4,5 の証明には以下の整数論からの事実が必要である。

Fact 6 $a,b\in\mathfrak{O}\setminus\{0\}$ とし，$\mathfrak{p}$ を素イデアル，m を $\mathfrak{p}^m\not|2$ なる自然数とする。もし $a\not\equiv 0\pmod{\mathfrak{p}^2}$ かつ $a\equiv b\pmod{\mathfrak{p}^{2m}}$ ならば a,b は同じ $\mathfrak{p}$*-adic class* に属している (つまり $a/b\in F_{\mathfrak{p}}^2$)。

Fact 7 $a, b \in \mathfrak{O} \setminus \{0\}$ とする。もし $(a,b)_{\mathfrak{p}} = -1$ ならば $\mathfrak{p}$ は *Archimedean valuation* かまたは $2ab$ を割る素イデアルである。従って $(a,b)_{\mathfrak{p}} = -1$ となる *valuation* は有限個である。

ここで $(a,b)_{\mathfrak{p}}$ は Hilbert symbol である，つまり

$$(a,b)_{\mathfrak{p}} = \begin{cases} +1 & \text{if } ax^2 + by^2 = 1 \text{ is solvable in } F_{\mathfrak{p}}, \\ -1 & \text{otherwise.} \end{cases}$$

Fact 8 $a \in \mathfrak{O}$ として $a \| \mathfrak{p}$ （つまり $\mathfrak{p} | a$ で $\mathfrak{p}^2 \nmid a$）ならばある $b \in \mathfrak{O}$ があって $\mathfrak{p} \nmid b$ で $(a,b)_{\mathfrak{p}} = -1$.

Fact 9 $a, b \in F^*$ に対して，$(a,b)_{\mathfrak{p}} = -1$ となるのは偶数個の *valuation* に対してである。

Fact 10 各イデアル類（*ideal class*）には無限個の素イデアルがある。

ideal class とは F の 0 イデアルと異なる分数イデアル全体のなす群を 0 イデアルと異なる単項分数イデアルのなす部分群で割った剰余群の各類のことである。

Fact 11 $a \in \mathfrak{O}$ がイデアル $\mathfrak{m}$ と互いに素ならば，$p \equiv a \pmod{\mathfrak{m}}$ であるような総正（*totally positive*）な素元 p が無限個ある。

Fact 12 $h \in F^*$ が F で $x^2 - ay^2 - bz^2$ の形に表わされる $\iff (a,b)_{\mathfrak{p}} = -1$ であるような $\mathfrak{p}$ に対して h が $-ab$ と同じ $\mathfrak{p}$-*adic class* に属さない。

Proof of Lemma 4. $\mathfrak{p}_1, \ldots, \mathfrak{p}_{2k-1}$ を 2 の素因子すべてを含む相異なる素イデアルの集合とする。$\mathfrak{K}$ を積 $\mathfrak{p}_1 \cdots \mathfrak{p}_{2k-1}$ を含む ideal class とする。Fact 10 より各 $\mathfrak{p}_i$ と異なる $\mathfrak{p}_{2k}$ を ideal class $\mathfrak{K}^{-1}$ から取る事ができる。すると $\mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$ は単項イデアルである。a をその生成元とする。つまり，$(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$.

次に b を決める。Fact 8 より，各 $i = 1, \ldots, 2k$ に対して $\mathfrak{O}$ から b_i を $\mathfrak{p}_i \nmid b_i$ で $(a, b_i)_{\mathfrak{p}_i} = -1$ であるように取れる。m をすべての素イデアル $\mathfrak{p}$ に対して $\mathfrak{p}^m \nmid 2$ となる自然数とする。Fact 6 より，もし

$$x \equiv b_i \pmod{\mathfrak{p}_i^{2m}} \quad \text{for } i = 1, \ldots, 2k$$

ならば x と b_i は同じ $\mathfrak{p}_i$-adic class に入るので，各 i に対して $(a,x)_{\mathfrak{p}_i} = -1$ である。Chinese Remainder Theorem より，上の連立合同式は $\mathfrak{p}_1^{2m} \cdots \mathfrak{p}_{2k}^{2m}$ を法としてただ 1 つの解 $c \in \mathfrak{O}$ を持つ。c は $\mathfrak{p}_1^{2m} \cdots \mathfrak{p}_{2k}^{2m}$ と互いに素である。Fact 11 より，

$$p \equiv c \pmod{\mathfrak{p}_1^{2m} \cdots \mathfrak{p}_{2k}^{2m}}$$

なる totally positive prime number $p \in D$ が無限個ある。そのうちの1つを b とする。c は a と互いに素であるから，b も a と互いに素である。

あと $(a,b)_{\mathfrak{p}} = -1 \iff \mathfrak{p}|a$ である事を示す。まず作り方より，再び Fact 6 より，$i = 1, \ldots, 2k$ に対して $(a,b)_{\mathfrak{p}_i} = -1$ である。b は総正だからすべての Archimedean valuation $\mathfrak{p}$ に対して $(a,b)_{\mathfrak{p}} = +1$ である。Fact 7 より $(a,b)_{\mathfrak{p}} = -1$ となりえる valuation は a を割るもの以外は $\mathfrak{p} = (b)$ だけである。しかし Fact 9 よりこれはありえない。よっていえた。 □

Remark 13 上の証明から分かるように，$(a,b)_{(b)} = +1$ である。これを次節で使う。

Proof of Lemma 5. 一般に F の元 c は共通の素因子を持たないような $u, v \in D, v \neq 0$ で $c = u/v$ と表わせる。よってこのような u, v に対して，

$$F \models \exists x, y, z(v^{2m} - abu^{2m} = x^2 - ay^2 - bz^2) \textit{ iff } v \textit{ is prime to } a$$

を示す。

$h = v^{2m} - abu^{2m}$ とおく。Fact 12 より，
$F \models \exists x, y, z(v^{2m} - abu^{2m} = x^2 - ay^2 - bz^2)$ *iff* $i = 1, \ldots, 2k$ に対して，h は $-ab$ と同じ $\mathfrak{p}_i$-adic class に入らない，
が成り立つ。

ある i で $\mathfrak{p}_i|v$ とする。$\mathfrak{p}_i$ は u や b を割らないから，

$$h \not\equiv 0 \pmod{\mathfrak{p}_i^2}, \quad h \equiv -abu^{2m} \pmod{\mathfrak{p}_i^{2m}}$$

である。Fact 6 より，h は $-abu^{2m}$ と同じ $\mathfrak{p}_i$-adic class に入っている。この class は $-ab$ の class と同じである。従って h は $x^2 - ay^2 - bz^2$ の形では表わせない。

逆に v は a と互いに素であるとする。すると h は a と互いに素であり，$\mathfrak{p}_i$ が丁度きっかり一度だけ ab を割る事より，h と $-ab$ とは同じ $\mathfrak{p}_i$-adic class には入らない。従って h は $x^2 - ay^2 - bz^2$ の形で表わせる。 □

Remark 14 上の証明は，

1. $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$，ここで各 $\mathfrak{p}_i$ は相異なり，2 の素因子をすべて含む。
2. b は a と互いに素で，$(a,b)_{\mathfrak{p}} = -1 \iff \mathfrak{p}|a$.

である事だけを使っている。これを次節で使う。

3 Theorem 2の無限次代数拡大体への拡張

lを奇素数しζ_{l^n}を1の原始l^n乗根とする。$F_0=\mathbb{Q}$, $n>0$に対して$F_n=\mathbb{Q}(\zeta_{l^n})$として, $K_l=\bigcup_n F_n$とおくと, $F_0\subset F_1\subset F_2\subset\cdots$であり, K_lは$\mathbb{Q}$の無限次Abel拡大である。$\mathfrak{O}_n$をF_nの代数的整数環とすればK_lの代数的整数のなす環は$\mathfrak{O}_{K_l}=\bigcup_n \mathfrak{O}_n$である。本節ではTheorem 15を証明する。

Theorem 15 次の*formula*を$\varphi(a,b,c)$で表わす。

$$\exists x,y,z(1-abc^4=x^2-ay^2-bz^2)$$

さらに$\psi(t)$は次の*formula*を表わす事にする。

$$\forall a,b(\forall c(\varphi(a,b,c)\to\varphi(a,b,c+1))\to\varphi(a,b,t))$$

すると$\mathbb{Z}\subseteq\psi(K_l)\subseteq\mathfrak{O}_{K_l}$である。

証明には次の円分体に関する事実を使う。

Fact 16 $0<i<j$とし, $\mathfrak{p}$をF_iの素イデアルとする。

1. $\mathfrak{p}\nmid l$ならば, $\mathfrak{p}$のF_jでの素因子分解は, $\mathfrak{p}=\mathfrak{P}_1\cdots\mathfrak{P}_g$. ここで$g$は$[F_j:F_i]=l^{j-i}$の約数である。

2. $\mathfrak{p}|l$ならば, $\mathfrak{p}$のF_jでの素因子分解は, $\mathfrak{p}=\mathfrak{P}^{l^{j-i}}$. ここで$\mathfrak{p}=(1-\zeta_{l^i})$, $\mathfrak{P}=(1-\zeta_{l^j})$である。

Fact 17 一般に次のことが成り立つ。

1. $(a_1a_2,b)_\mathfrak{p}=(a_1,b)_\mathfrak{p}(a_2,b)_\mathfrak{p}$

2. K,kを数体とし, $K_\mathfrak{P}/k_\mathfrak{p}$が有限次拡大, $b\in k_\mathfrak{p},\alpha\in K_\mathfrak{P},a=N_{K_\mathfrak{P}/k_\mathfrak{p}}(\alpha)$とすると, $(\alpha,b)_\mathfrak{P}=(a,b)_\mathfrak{p}$.

Lemma 18 $0<i<j$とし, $a,b\in F_i$, $\mathfrak{p}$をF_iの素イデアルとし, $\mathfrak{P}$をF_jでの$\mathfrak{p}$の素因子とする。

$(a,b)_\mathfrak{p}=-1$ならば$(a,b)_\mathfrak{P}=-1$であり, $(a,b)_\mathfrak{p}=+1$ならば$(a,b)_\mathfrak{P}=+1$である。

Proof. ここで $0 < i < j$ とすると，$(F_j)_{\mathfrak{p}}/(F_i)_{\mathfrak{P}}$ は次数が $[F_j : F_i] = l^{j-i}$ を割り切る有限次拡大である。次数を u とすると $N_{(F_j)_{\mathfrak{P}}/(F_i)_{\mathfrak{p}}}(a) = a^u$ だから，上の事実より $(a,b)_{\mathfrak{P}} = (a,b)_{\mathfrak{p}}^u$ となる。u は奇数よりいえた。 □

Proof of Theorem 15. $\mathbb{Z} \subseteq \psi(K)$ は明らかである。今 $t \in K \setminus \mathfrak{O}_K$ を取る。この t に対して，ある $a, b \in K_l$ があり，

$$K_l \models \neg\varphi(a,b,t) \wedge \forall c(\varphi(a,b,c) \to \varphi(a,b,c+1))$$

であることを示せばよい。

t を含む F_n を1つ固定する。$n > 1$ に取る。

するとある F_n の素イデアル $\mathfrak{p}_1$ に対して，t は $\mathfrak{p}_1$-adic integer ではない。この $\mathfrak{p}_1$ に対して Lemma 3 を適用して，$\mathfrak{O}_n$ から a, b を取る。

1. $(a) = \mathfrak{p}_1 \cdots \mathfrak{p}_{2k}$，ここで各 $\mathfrak{p}_i$ は相異なり，2 の素因子をすべて含む。

2. b は totally positive prime number in $\mathfrak{O}$ で，$(a,b)_{\mathfrak{p}} = -1 \iff \mathfrak{p}|a$.

であるが，$\mathfrak{p}_2, \ldots, \mathfrak{p}_{2k}$ の各素因子は素数 l を割らないように取れる。

F_n では Fact 16 より，すべての素イデアル $\mathfrak{p}$ に対して $\mathfrak{p}^2 \not| 2$ だから前節の Lemma 5 より $1 - abt^4 = x^2 - ay^2 - bz^2$ は解 x, y, z を F_n に持たない。

この a, b に対して，$1 - abt^4 = x^2 - ay^2 - bz^2$ が K_l で解を持たないこと，及び $c \in K_l$ が解なら $c+1$ も解であることを示せばよい。

$s > n$ として，$1 - abt^4 = x^2 - ay^2 - bz^2$ が F_s でも解 x, y, z を持たない事，及び $c \in F_s$ が解ならば $c+1$ も解であることをいえばよい。$s - n$ を偶数に取ってもよい。

case 1. $\mathfrak{p}_1$ が素数 l の素因子でないとき:

まず $a, b \in \mathfrak{O}_s$ で a と b は $\mathfrak{O}_n$ で互いに素であるから，$\mathfrak{O}_s$ でも互いに素である。

Fact 16 より F_s での素因子分解は，

1. $(a) = \mathfrak{P}_1 \cdots \mathfrak{P}_{2r}$，ここで各 $\mathfrak{P}_i$ は相異なり，2 の素因子をすべて含む。

となる。

Remark 13 と Lemma 18 より

2. a と b は $\mathfrak{O}_n$ で互いに素で，$(a,b)_{\mathfrak{P}} = -1 \iff \mathfrak{P}|a$.

がいえる。Remark 14 より，m を 2 とした Lemma 5 が F_s で成り立ち，同じようにして，$1 - abt^4 = x^2 - ay^2 - bz^2$ は解 x, y, z を F_s に持たない。

$c \in F_s$ が解ならば $c+1$ も解であることも明らかである。

case 2. $\mathfrak{p}_1$ が素数 l の素因子であるとき:

Fact 16 より F_s での a の素因子分解は,

1. $(a) = \mathfrak{P}_1^{l^{s-n}} \cdots \mathfrak{P}_{2r'}$, ここで各 $\mathfrak{P}_i$ は相異なり, 2 の素因子をすべて含む。

となる。Fact 16 より $\mathfrak{P}_1 = (1-\zeta_{l^s})$ である。$a' = a/(1-\zeta_{l^s})^{l^{s-n}-1}$ とおくと,

1. $(a') = \mathfrak{P}_1 \cdots \mathfrak{P}_{2r'}$, ここで各 $\mathfrak{P}_i$ は相異なり, 2 の素因子をすべて含む。

次に $a = a'((1-\zeta_{l^s})^{(l^{s-n}-1)/2})^2$ より, 各 i に対して $(a,b)_{\mathfrak{P}_i} = (a',b)_{\mathfrak{P}_i}$ である。
($(l^{s-n}-1)/2$ は整数。) また $\mathfrak{O}_s = \bigcap_{\mathfrak{P}} \mathfrak{O}_{\mathfrak{P}}$ より $a' \in \mathfrak{O}_s$.

よって,

2. a' と b は $\mathfrak{O}_s$ で互いに素で, $(a',b)_{\mathfrak{P}} = -1 \iff \mathfrak{P}|a'$.

従って同様に,

$1 - a'bc^4 = x^2 - a'y^2 - bz^2$ は解 x,y,z を F_s に持つ $\iff$ c は $\mathfrak{P}|a'$ なる $\mathfrak{P}$ に対して $\mathfrak{P}$-adic integer, が成り立つ。

今 $1 - abt^4 = x^2 - ay^2 - bz^2$ が解 x,y,z を F_s に持つとする。$s-n$ が偶数より $(l^{s-n}-1)/4$ は整数だから,

$$1 - a'b(t(1-\zeta_{l^s})^{(l^{s-n}-1)/4})^4 = x^2 - a'((1-\zeta_{l^s})^{(l^{s-n}-1)/2}y)^2 - bz^2$$

が解 x,y,z を F_s に持つことになる。しかし $t(1-\zeta_{l^s})^{(l^{s-n}-1)/4}$ は、$\mathfrak{p}_1 = \mathfrak{P}_1^{l^{s-n}}$ であることに注意すれば, $\mathfrak{P}_1$ に対して $\mathfrak{P}_1$-adic integer にならないから矛盾する。よってこのときも $1 - abt^4 = x^2 - ay^2 - bz^2$ は解 x,y,z を F_s に持たない。

次に, $c \in F_s$ が $1 - abt^4 = x^2 - ay^2 - bz^2$ の解ならば $c+1$ も解であることを示す。$c \in F_s$ が解とする。すると, $c(1-\zeta_{l^s})^{(l^{s-n}-1)/4}$ は,

$$1 - a'bt^4 = x^2 - a'((1-\zeta_{l^s})^{(l^{s-n}-1)/2}y)^2 - bz^2$$

の解である。よって, $c(1-\zeta_{l^s})^{(l^{s-n}-1)/4}$ は $\mathfrak{P}|a'$ なる $\mathfrak{P}$ に対して $\mathfrak{P}$-adic integer である。このとき, 附値の計算により, $(c+1)(1-\zeta_{l^s})^{(l^{s-n}-1)/4}$ も $\mathfrak{P}|a'$ なる $\mathfrak{P}$ に対して $\mathfrak{P}$-adic integer である。したがって, $c+1$ も $1 - abt^4 = x^2 - ay^2 - bz^2$ の解である。□

4 おわりに

無限次代数体 K_l では Theorem 15 がいえてもそこから $\mathfrak{O}_K$ の definability を導くのは, 有限次代数体のように簡単ではない。

しかし，有限次代数体のときと同じアイデアを用いて，$\mathfrak{O}_{K_l}$ に含まれる，F_n を含む definable subset を構成できる。

今，ζ_{l^n} の $\mathbb{Q}$ 上の最小多項式 (円周多項式) を $P(x)$，$s = l^{n-1}(l-1)$ として $\tilde{\psi}_n(t)$ を，

$$\exists x_1, \ldots, x_s, y(t = x_1 + x_2 y \cdots + x_s y^s \wedge P(y) \wedge \bigwedge_i \psi(x_i))$$

とすると，明らかに，

$$F_n \subseteq \tilde{\psi}_n(K_l) \subseteq \mathfrak{O}_{K_l}$$

である。

$\mathfrak{O}_{K_l} = \bigcup_n \tilde{\psi}_n$ であるから，

Corollary 19 *K_l では，非代数的整数の集合は infinity-definable である。しかも，定義する partial type は recursive である。*

J.Robinson (と Raphael Robinson) は，[1] の中で，次の lemma と inductive form の考えを用い，一般の (有限次) 代数体 F の代数的整数環 $\mathfrak{O}_F$ の中で，自然数全体の集合 $\mathbb{N}$ が -definable であることを示した。

Lemma 20 *$n = [F : \mathbb{Q}]$, f を 0 でない F の任意の数としたとき，*

$$a+1|f \wedge a+2|f \wedge \cdots \wedge a+n|f$$

となるような $a \in \mathfrak{O}_F$ は有限個である。

Proof. $S = \{a \in \mathfrak{O}_F : \bigwedge_i a+i|f\}$, $T = \{P_a(x) \in \mathfrak{O}_F[x] : P_a(x) = (x + a^{(1)}) \cdots (x + a^{(n)})\}$ とおく。ここで $a^{(1)}, \ldots, a^{(n)}$ は a の F における共役元である。f の絶対ノルム $N(f)$ は 0 でないことより，有限個の素数の積である。$N(a+k)$ が $N(f)$ を割ることより，$U_k = \{N(a+k) : a \in S\}$ は有限集合である。(ここで $k = 1, \ldots, n$) $P_a(x)$ は monic な次数 n の多項式であるから，$P_a(1), \ldots, P_a(n)$ によって一意に定まる。

一方 $N(a+k) = P_a(k)$ である。したがって，T は有限集合である。$P_a(-a) = 0$ より，S も有限集合である。 □

そこで，$\tau(a, f, g, h)$ を，

$$f \neq 0 \wedge a+1|f \wedge a+2|f \wedge \cdots \wedge a+n|f \wedge 1+ag|h$$

とし，$\theta(t)$ を，

$$\exists f, g, h\,[\tau(0, f, g, h) \wedge \forall a\,(\tau(a, f, g, h) \rightarrow a = t \vee \tau(a+1, f, g, h))]$$

とすると，$\theta(t)$ は $\mathfrak{O}_F$ のなかで $\mathbb{N}$ を定義する。

前の lemma と inductive form の考えにより，$\theta(\mathfrak{O}_F) \subseteq \mathbb{N}$ はすぐに出る。逆を示すとき，$1+ag|h$ を用いる。

このアイデアを用いて，K_l の中で，$\mathbb{N}$ を除外する formula を構成できる。今，$\tilde{\tau}(a,f)$ を，

$$f \neq 0 \wedge a+1|f \wedge a+2|f \wedge \cdots \wedge a+l-1|f \wedge \psi(a) \wedge \psi(f)$$

とする。

$[F_1 : \mathbb{Q}] = l-1$ であり，lemma 20 では f が $\mathfrak{O}_F$ 以外の代数的整数でもよいことに注意すれば（ただし $|$ は大きな代数体の中で割れるという意味にする．），

$\tilde{\theta}(t)$ を，

$$\exists f\,[\tilde{\tau}(0,f) \wedge \forall a\,(\tilde{\tau}(a,f) \rightarrow a = t \vee \tilde{\tau}(a+1,f))]$$

とおくと（ここで $a|b$ は $\exists c(a = bc \wedge \psi(c))$ とする。），

Proposition 21 $\tilde{\theta}(t)$ は K_l の中で，$\mathbb{N}$ を除外する。つまり $\tilde{\theta}(K_l) \subseteq \mathbb{N}$ である。

実際，$K_l \models \tilde{\theta}(t)$ で $t \notin \mathbb{N}$ とすると，K_l の中で，$\tilde{\tau}(0,f), \tilde{\tau}(1,f), \ldots$ となり，F_1 に対する lemma 20（f が $\mathfrak{O}_1$ 以外の場合）に反する。

しかし，$\tilde{\tau}(t)$ を知ることは困難である。空集合かどうかも調べることは困難である。

Theorem 15 の奇素数以外への拡張も難しい。2^n 分体の tower K_2 に対しては，Robinson の formula は適用できない。各 F_n で 2 が次数いっぱいに分岐するため m が一様に取れない。一方 2 を素因子に含まない自然数 n をとって作る n^k 分体の tower に対してもそのままでは無理である。

参考文献

[1] Robinson, J., *The undecidability of algebraic rings and fields*, Proc. Amer. Math. Soc., 10, pp 950-957, 1959.